Système informatique de P&rl

VERSION : 1
Date : 19.06.2020

Examens
2020

Certificat d'administrateur système et réseaux

IDEC, Renens

Documentation du
système informatique de P&rl
Conçu par *Alain Philip Despont*

Sommaire

Concept global de P&rl

P&rl est constitué d'une arborescence traditionnelle pour une entreprise ; elle comporte une direction, des secrétaires chargées de traiter les demandes des clients, un service marketing, un service comptabilité, des commerciaux chargés de trouver des entreprises pour étoffer le catalogue de prestation de P&rl, ainsi que des « perles spécialistes » de leur domaines, en l'occurrence le nettoyage de voiture, l'organisation d'anniversaire, de réceptions...

Finalement, P&rl possède un embryon de service informatique, qui a quelques droits pour entretenir et sauvegarder le système de l'entreprise.

En dehors des « perles administratives » spécialistes et autres perles au fonctions bien définies, la plupart des activités sont effectuées par des perles de base, ayant accès aux seules ressources nécessaires à leur fonction.

Lignes directrices

Chaque « perle » doit pouvoir accéder en tout temps et tout lieu, aux contrats et catalogue de prestation, ainsi qu'aux données clients pour l'exécution de leur tâches.

Les « perles » administratives doivent êtres restreintes dans leur activité respective, aucune entreprise ne saurait tolérer que de quiconque puisse accéder à la comptabilité, documents bancaires ou dossiers du personnels (par exemple).

Cela vaut également pour le membres du service informatique qui doivent pouvoir sauvegarder le système et pouvoir effectuer un travail de bureau, sans pour autant pouvoir accéder a des dossiers et fichiers sensibles.

P&rl préservera les communications avec les clients, aux « perles administratives » concernées.

Service informatique interne

Pour que P&rl reste maîtresse de la plupart des fonctions informatiques, tout en restant protégée de la malveillance possible d'un des membre du service informatique, les rôles suivants ont étés distribués au groupe des informaticiens :

- Opérateur d'impression ; peut gérer les problématiques liées aux imprimantes.
- Opérateur de sauvegarde ; pour gérer les sauvegardes régulières et rétablir le service dans les plus brefs délais.
- Délégation de contrôle, permettant de créer et supprimer des comptes sur le domaine, et ce, sans pouvoir modifier les groupes internes. Ils peuvent cependant ajouter et supprimer des perles. L'ajout d'un membre administratif se fera donc sur demande, par l'administrateur du système, afin de limiter tout abus.

Limites d'application

La documentation du système se limites aux postes de travail et serveurs sous contrôle direct de P&rl, utilisateurs, ressources et groupes définis sur le système interne de l'entreprise, ainsi que les liens et communications avec des serveurs et/ou équipements annexes si besoin.

La documentation ne traite pas du site web ou toute autre structure extérieure à Perl.

Serveurs et systèmes clients de P&rl

P&rl possède un serveur Active Directory faisant office de DNS, ainsi qu'un serveur contrôleur de domaine pour la tolérance de panne. Le serveur PERL1 a aussi pour rôle de distribuer les adresses IP aux utilisateurs du réseau à l'aide de la fonctionnalité DHCP, et DHCP est configuré pour basculer sur PERL2 si besoin. Les systèmes clients eux sont basés sur Windows 10 et leurs fonctionnalités sont limitées par l'usage des GPO.

Le tout fait partie du domaine : **PERL.local**

Serveurs de P&rl

Nom d'hôte netbios	Rôles activés	Fonctionnalités activées
[PERL1] **WIN-JR71JL8EBKC**	Active Directory (AD), DNS, DHCP, Fichiers	Sauvegarde windows
[PERL2] **WIN-HVFUCDP6E52**	Active Directory (DC), DNS, DHCP, Fichiers	Sauvegarde windows

Système d'exploitation	Microsoft Windows Server 2016 Datacenter
Dernière mise à jour	Le 30.03.20
Clé de produit	HFGTK-NQ8FG-R7344-XJQDH-94T3H
Groupe de travail ou Nom de domaine	PERL.local
Dossier de la base de donnée	C:\WINDOWS\NTDS
Dossier des fichiers journaux	C:\WINDOWS\NTDS
Dossier SYSVOL	C:\WINDOWS\SYSVOL

Adresse des serveurs sur le réseau

Adresse IP (fixe)	PERL1 : 192.168.0.10 PERL2 : 192.168.0.11
Masque de sous réseau	255.255.255.0
Passerelle par défaut	192.168.0.150
Serveur DNS préféré	PERL1 : 192.168.0.10 / 192.168.0.11 PERL2 : 192.168.0.11 / 192.168.0.10

Systèmes clients de P&rl

COMPTE ADMIN	Admin1 / Passw0rd
Système d'exploitation	Microsoft Windows 10 Education v1511
Dernière mise à jour	KB4551762 (le 29.03.2020)
Clé de produit	YF4NH-QXYX4-RJXKT-F6F64-W8F8D

Configuration du réseau et étendues DHCP

P&rl utilise une seule étendue DHCP pour distribuer les adresses IP sur le réseau, mais plusieurs réservations fixes, principalement pour les serveurs du domaine (PERL1 et PERL2).

PERL1 est le serveur DHCP par défaut, et en cas de problème ou pour la maintenance, le rôle bascule sur PERL2.

Plages d'adresses configurées

Nom de la plage	Adresse de début	Adresse de fin	Masque de sous-réseau
Adresses PERL	192.168.1.30	192.168.1.100	255.255.255.0

Configuration du DHCP

Durée du bail : 2 jours (8jours par défaut)

Domaine parent : PERL.LOCAL

Adresse IP du serveur DNS : 192.168.0.10 / 192.168.0.11

Options de serveur : Activé

Options d'étendues : Aucune activée

Options de réservations (IP Fixes)

Nom de la réservation	Description	Addresse IP	Adresse MAC
PERL1	Serveur AD	192.168.0.10	00-15-5D-00-66-44
PERL2	Serveur DC	192.168.0.11	00-15-5D-00-66-47

Prévision sur l'utilisation des adresses IP

L'entreprise P&rl compte actuellement une quinzaine d'employés fixes, et un nombre indéterminé d'employés ayant le statut de « perle » uniquement.

Selon la charge de travail, on peut compte que P&rl n'aura pas besoin d'une plage d'adresse plus conséquente avant un moment, puisque :

1 : Les perles administratives sont peu nombreuses (15-20).

2 : Les perles simples ne travaillent pas tous les jours.

Actuellement la plage d'adressage DHCP permet de donner une adresse IP à plus de 70 clients en même temps, ce qui inclus la quinzaine d'employés fixes, une cinquantaines de perles possibles, ainsi que 16 serveurs (192.168.1-9 et .12-19) et 9 imprimantes (192.168.0.21-30) si les besoins augmentent.

Liste des ressources, partages et points de partages

Les documents, données, et dossier partagés de l'entreprise P&rl sont stockés sur un NAS, dans les bureaux de l'entreprise. Une partie des données de vente et marketing sont en copie sur l'hébergement web du site internet « vitrine ».

Racines des dossiers			o/n	Nom du partage	Contenu
NAS$				\\WIN-JR71JL8EBKC\NAS$	
	Applications				Package d'applications à distribuer
	Sauvegardes				Sauvegardes des serveurs
		PERL1	**O**	\\WIN-JR71JL8EBKC\Perl1	
		PERL2	**O**	\\WIN-JR71JL8EBKC\Perl2	
	Dossiers administratifs				Destinés aux perles administratives.
	Administratif				Documents bancaires, fiscaux
		Banque			
		Impôts			
		AVS			*RH a besoin de lire*
		Courrier			
	Comptabilité				Données comptables, factures
		Factures			
		Salaires			*RH a besoin de lire*
	Marketing				Documents de promotion de l'entreprise
		Modèles			
		Pages web			
		Publicité			
	RH				Documents relatifs au personnel
	Satisfaction				Enquêtes de satisfaction et réclamations
		Enquêtes			
		Réclamations			*RH a besoin de lire*
		Suivis			
	Dossiers perles				Destinées aux simples perles
	Clients				Coordonnées des clients et courrier
		Données			Coordonnées des clients
		Courriers			Correspondance avec les clients
	Mandats				Description des travaux demandés par les clients
	Vente				Devis, contrats et catalogue
		Modèles			
		Contrats			
		Catalogue			

Partages administratifs de PERL1

\\WIN-JR71JL8EBKC\C$	Lecteur du système de PERL1
\\WIN-JR71JL8EBKC\IPC$	Communications inter-processus pour contrôle à distance
\\WIN-JR71JL8EBKC\NETLOGON$	Copie des fichiers publics du domaine pour réplication
\\WIN-JR71JL8EBKC\SYSVOL$	Scripts de connexion au domaine et GPO qui seront répliquées sur le contrôleur de domaine.
\\WIN-JR71JL8EBKC\PRINT$	Lien direct aux imprimantes
\\WIN-JR71JL8EBKC\NAS$	Lien direct vers le NAS de P&rl
\\WIN-JR71JL8EBKC\ADMIN$	Lien direct à certains outils d'administration
\\WIN-JR71JL8EBKC\Users	

Dossiers partagés

\\WIN-JR71JL8EBKC\Perl1	Sauvegarde windows server de PERL1 (limité aux opérateurs de sauvegarde et Admin.).
\\WIN-JR71JL8EBKC\Perl2	Sauvegarde windows server de PERL2 (limité aux opérateurs de sauvegarde et Admin.).

Imprimantes partagées du domaine

P&rl possède une imprimante, mais les utilisateurs peuvent, selon leur droits, utiliser plusieurs configurations prédéfinies. Le fax est accessible 24h/24h.

Partage	Type	Horaire	Priorité	Accès	IP	Emplacement
\\WIN-JR71JL8EBKC**Brother Couleur**	Couleur	8h-18h	99	Sauf Perles	192.168.0.20	Bureau
\\WIN-JR71JL8EBKC**Brother Noir**	Noir	8h-18h	98	TOUS	192.168.0.20	Bureau
\\WIN-JR71JL8EBKC**Brother Fax**	Noir	24h	97	TOUS	192.168.0.20	Bureau

Politique de sécurité générale

Seul l'administrateur principal peut modifier ou accéder aux configurations des serveurs, et l'ajout d'un utilisateur à un groupe global reste sa prérogative. Le service informatique fait partie des Opérateurs de sauvegarde et d'impression, il a une délégation de contrôle sur l'UO « Utilisateurs » permettant de créer, supprimer des comptes, et réinitialiser les mots de passe si besoin. Il peut également ajouter et supprimer des membres au groupe des perles.

Problèmes sécuritaires et de fonctionnalités connus

Rôles FSMO divisés sur les deux contrôleurs (PDC + rôle inconnu, sur PERL1) qui ont besoin d'être en service en même temps, possible problèmes de réplications. **Noms d'hôtes** pas conséquents : doit renommer. **OpenOffice** semble ne pas s'installer. **DHCP désactivé** sur Win10, IP fixée a cause de déconnexion au domaine (DNS) de dernière minute.

Politique et fréquences des sauvegardes

La sauvegarde complète à l'aide de la sauvegarde windows (Fonctionnalité) est configurée, et les sauvegardes des serveurs sont stockées sur le NAS.

Sauvegarde complète	Chaque jour	A minuit

Plans de restauration du système

Lorsque PERL1 tombe en panne

PERL2 prends le relais en tant que DC, et DHCP. Le système de PERL1 pourra être restauré sans empêcher le travail.

Lorsque une panne survient sur un des serveur PERL1 ou PERL2

L'opérateur de sauvegarde peut restaurer le système via la console Sauvegarde Windows Server en reprenant une des sauvegarde disponible sur le NAS.

Politique d'audit du système

Pour vérifier les accès au serveurs et modifications sur le domaine via le journal d'événement windows, une stratégie de groupe spéciale de sécurité a été créé pour :

- Auditer les événements de connexion aux comptes qui ont ECHOUEES à se connecter sur le domaine.
- Auditer la gestion des comptes REUSSIE, en cas de modification d'un compte.
- Auditer les événement de connexions des utilisateurs qui ont REUSSI ou ECHOUES a se connecter a un des contrôleurs de domaine.

Emplacement des journaux systèmes

Les journaux d'événements du système se trouvent sur :
%SystemRoot%\System32\Winevt\Logs et leur archivage doit être fait manuellement.

Arborescence du domaine et application des stratégies des groupes du domaine

L'entreprise P&rl possède un seul domaine : **PERL.local**				
Arborescence des OU / (D) = Délégation de contrôle pour service informatique				**Stratégies de groupes sur l'UO**
PERL.local				Default Domain Policy
	Domain Controllers			Default Domains Controller Policy GPO_Securite_Audit
	PERL			
		Utilisateurs (D)		GPO_Deploy_LecteurMappé
			Administratifs	GPO_Deploy_PDF
			Perles	
		Clients		
			Serveurs	
			Postes fixes	GPO_Deploy_OpenOffice GPO_FirewallOpen_UDP4333 GPO_Deploy_Imprimantes
			Postes mobiles	GPO_Deploy_OpenOffice GPO_FirewallOpen_UDP4333 GPO_Deploy_Imprimantes
		Imprimantes		
		Partages		

Descriptions des stratégies de groupe du domaine « PERL.local »

Liste complète des stratégies de groupes présentes sur le domaine. Se référer à la page précédente pour le niveau ou elles sont appliquées.

Default Domain Policy	Spécifie des règles d'accès au domaine (Par défaut)
Default Domains Controller Policy	Spécifie des règles d'accès au serveurs contrôleurs de domaine (Par défaut)

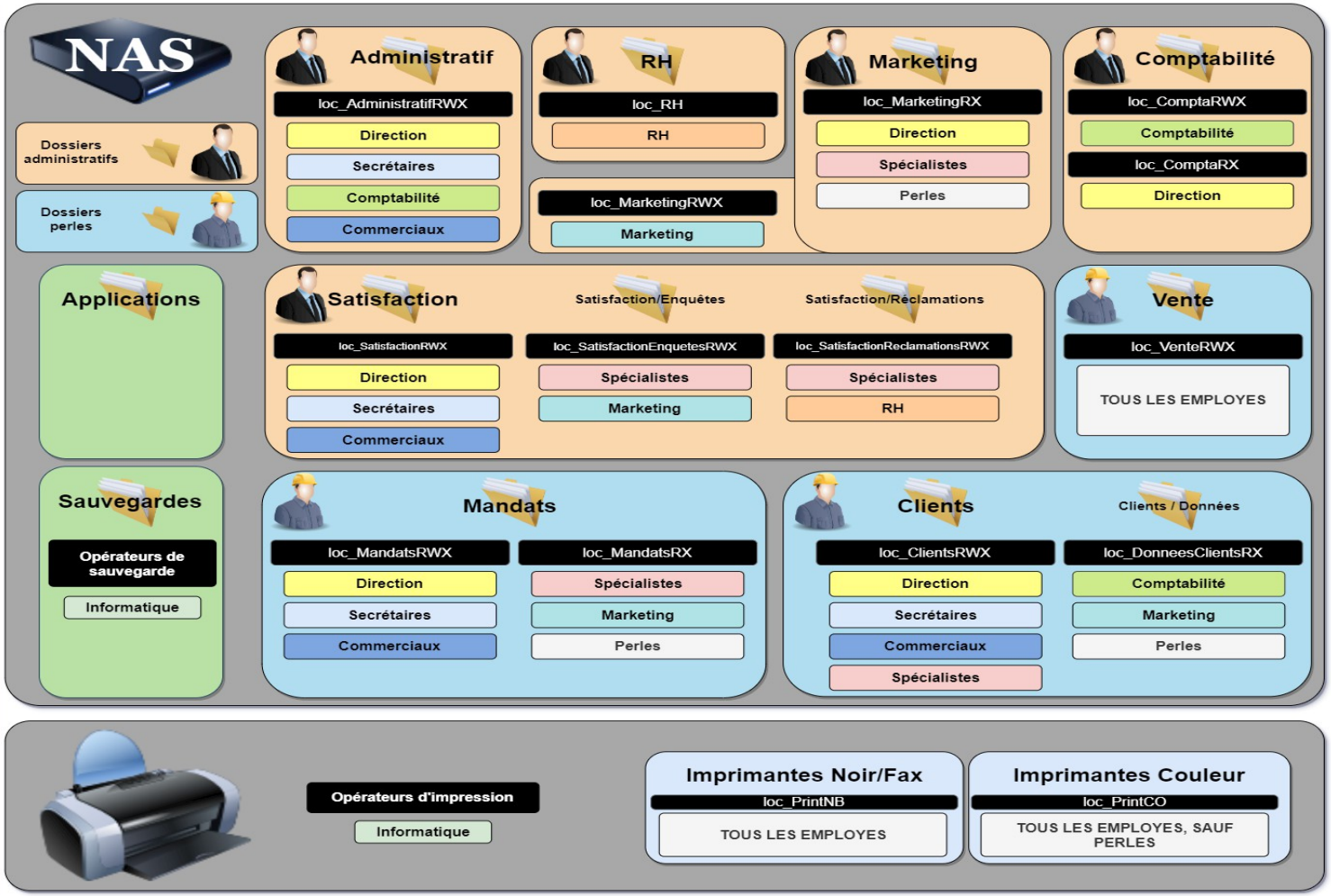
GPO_Securite_Audit	Audit les événements de connexion, la gestion des comptes et les événement de connexions des utilisateurs au domaine.
GPO_Firewall_Open_UDP4333	Ouvre le port UDP 4333 sur tous les postes fixes et mobiles, afin d'accéder au serveur de GRH ***4333:UDP :*:enabled:PortServeurGRH***
GPO_Deploy_PDF	Déploie PDF24 aux « perles administratives »
GPO_Deploy_OpenOffice	Déploie OpenOffice chez tous les postes se connectant au domaine.
GPO_Deploy_Imprimantes	Déploie les imprimantes du domaine chez les utilisateurs
GPO_Deploy_LecteurMappé	Déploie un lecteur réseau X aux perles administratives, et Y aux perles normales, afin d'avoir accès a leur partages respectifs.

Ressources et droit d'accès des groupes globaux d'utilisateurs du domaine

Groupes globaux ->	Direction	Spécialistes	Commerciaux	Secrétaires	Comptabilité	Informatique	Marketing	Ressources Humaines	Perles	Groupes locaux
Administratif	**RWX**			**RWX**	**RWX**			>Afficher<		**loc_AdministratifRWX**
Banque										
Impôts										
AVS								**RX**		
Courrier										
Clients	**RWX**	**RWX**	**RWX**	**RWX**	>Afficher<		>Afficher<		>Afficher<	**loc_ClientsRWX**
Données					**RX**		**RX**		**RX**	**loc_DonnéesClientRX**
Courriers										
Comptabilité	**RX**				**RWX**			>Afficher<		**loc_ComptaRWX / loc_ComptaRX**
Factures										
Salaires								**RX**		
Mandats	**RWX**	**RX**	**RWX**	**RWX**			**RX**		**RX**	**loc_MandatsRWX / loc_MandatsRX**
Marketing	**RX**	**RX**	**RX**				**RWX**			**loc_MarketingRWX / loc_MarketingRX**
Modèles										
Pages web										
Publicité										
RH								**RWX**		**loc_RH (AVS, Salaires, RH, Réclamations)**
Satisfaction	**RWX**	>Afficher<	**RWX**	**RWX**			>Afficher<	>Afficher<		**loc_SatisfactionRWX**
Enquêtes		**RWX**					**RWX**			**loc_SatisfactionEnquetesRWX**
Réclamations		**RWX**						**RWX**		**loc_SatisfactionReclamationsRWX**
Suivis										
Vente	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**loc_VenteRWX**
Modèles										
Contrats										
Catalogue										
ImprimanteNBFax	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**loc_PrintNB**
ImprimantesCO	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**	**RWX**		**loc_PrintCO**
Délégation pour gestion des comptes / Opérateurs de sauvegarde / Opérateur d'impression						**DGCOPSI**	**Peut ajouter des utilisateurs au groupe des Perles uniquement / Accès sur le dossier Sauvegardes du NAS**			

Groupes globaux et locaux du domaine

Paola Riggio-Liguri	glb_Direction
Hélène Divorne	glb_Spécialistes
Daniel Corrado	glb_Spécialistes
Marc Fourrier	glb_Commerciaux
Marco Patelli	glb_Commerciaux
Jack Baumann	glb_Secrétaires
Mina Maestro	glb_Secrétaires
Silvia Almeras	glb_Secrétaires
Hans Vieler	glb_Comptabilité
Yohann Ferreiro	glb_Informatique
Phil Legrand	glb_Informatique
Bernard De Rahm	glb_Marketing
Tara Kriegger	glb_Ressources Humaines
Alain Despont	glb_Perles



Listes des utilisateurs du système

Liste actualisée le 29.05.2020

Les comptes ont étés créés, avec le minimum d'informations requis (compte, prénom, nom, et mdp). Le service informatique peut compléter selon les besoins de l'entreprise.

Compte administrateur serveur : Administrateur / Passw0rd

Compte	Prénom	Nom	Email	Service	Description
PaRi1	Paola	Riggio-Liguri	paola.riggio@perl.ch	Administratif	Directrice de l'entreprise
HeDi1	Hélène	Divorne	helene.divorne@perl.ch	Administratif	Nettoyage de voitures
DaCo1	Daniel	Corrado	daniel.corrado@perl.ch	Administratif	Organisation d'anniversaires
MaFo1	Marc	Fourrier	marc.fourrier@perl.ch	Administratif	Cherche fournisseurs pour catalogue
MaPa1	Marco	Patelli	marco.patelli@perl.ch	Administratif	Cherche fournisseurs pour catalogue
JaBa1	Jack	Baumann	jack.baumann@perl.ch	Administratif	Traite les demandes client
MiMa1	Mina	Maestro	mina.maestro@perl.ch	Administratif	Traite les demandes client
SiAl1	Silvia	Almeras	silvia.almeras@perl.ch	Administratif	Traite les demandes client
HaVi1	Hans	Vieler	hans.vieler@perl.ch	Administratif	Gère la comptabilité
YoFe1	Yohann	Ferreiro	yohann.ferreiro@perl.ch	Administratif	Gère le SI
PhLe1	Phil	Legrand	phil.legrand@perl.ch	Administratif	Gère le SI
BeDe1	Bernard	De Rahm	bernard.derahm@perl.ch	Administratif	Marketing
TaKr1	Tara	Kriegger	tara.kriegger@perl.ch	Administratif	S'occupe de recruter les perles
AlDe1	Alain	Despont	alain.despont@perl.ch	Perle	Une vraie perle !